TOP SECRET "U"

Ticom/I-38

REPORT ON INTERROGATION OF LT. FROWEIN OF OKM/4 SKL III, ON HIS WORK ON THE SECURITY OF THE GERMAN NAVAL FOUR-WHEEL ENIGMA.

This interrogation was carried out on 21st June, 1945, at the OKM Signals School, FLENSBURG.

Lt. (MN)d.R. HANS-JOACHIM FROWEIN was attached to OKM/4 SKL II for six months from July 1944, to investigate the security of the Enigma.

Ticom
14 July, 1945

No. of pages 7
Copy No. 21

DISTRIBUTION:

British	
1	Director
2	D.D.3
3	D.D.4
4-9	D.D.(N.S.)(6)
10	D.D.(MW)
11	D.D.(A.S.)
12-13	A.D.(C.C.R.)(2)
14	Lt.Col. Leathem

TICOM	
15	Chairman
16-17	S.A.C.(2)
18	Cdr. Bacon
19	Cdr. MacKenzie
20	Cdr. Tandy
21	Lt.Col. Johnson
22	Lt.Cdr. Manson
23	Maj. Seaman
24	Lt. Eachus
25	Lt. Vance
26	Capt. Cowan
27	Lt. Fehl
28-29	Ticom Files(2)

U.S.	
30-31	OP20-G(2)(via Lt. Pendergrass)
32	G-2(via Lt.Col. Hilles)
33-34	S.S.A.(2)(via Major Seaman)
35	Director, S.I.D. ETOUSA(via Lt.Col. Johnson)

Additional:	
36	A.D.(Mch)
37	Dr. Plumb
38	Mr. C.H.O'D Alexander
39	S.A.C. for D.S.D.10 Admiralty

Subjects: Lt. FROWEIN 4 SKL III
C.R.R. TRANOW 4 SKL III

Present: Cdr. Dudley Smith, R.N.
Lt.Cdr. Forster, R.N.V.R.
Lt.Cdr. Davenport, R.N.V.R.

1. Oberregierungsrat TRANOW explained the reasons which lead up to Lt. FROWEIN's research work on the German Naval Enigma. They had suffered very heavy U-Boat losses in 1943 and early 1944 and an enquiry was ordered into the causes of this situation. It was suggested that these losses might be due to cypher messages to and from or concerning U-Boats being decyphered by the enemy. It was considered possible that an Enigma machine complete with drums and P/L copies of German signals might have been captured from a U-Boat. They were continually occupied with the consideration "Is the machine safe?". The operational authorities could not understand why boats were being sunk in certain positions.

2. An important consideration, however, was their knowledge of the allied D/F Code, from which they realised the very great part which D/F played in British and United States operations. The original British D/F Bearing Code had not been read but later the letter code which replaced it was broken easily.

3. It was decided that Lt. FROWEIN should be detached from 4 SKL III and lent to 4 SKL II for a period of six months, to carry out a comprehensive investigation into the security of the four-wheel Naval Enigma. He joined 4 SKL II in July 1944 and continued the work until January 1945. He started with a staff of two officers and ten men, but they were gradually taken away from him for other duties; at the end he only had two assistants left who were capable of doing other than "stooge" work.

4. Since signals from U-Boats were often very short, it was decided that the research should be based on having a known short crib of only 25 letters. They started from scratch, none of them had any knowledge or experience of breaking the Commercial Enigma, nor of any other cypher machine. At first they worked on the problem with no Stecker and then gradually increased the difficulties.

5. FROWEIN then proceeded to explain the details of the work; although the following account has been left in the first person, it does not represent a literal translation of his statements; it was not possible to take a full shorthand record of the conversation owing to the fact that most of it was based on rough diagrams made by him during the course of the explanation.

---

6. The basis of my work was the knowledge which an unauthorised person might be expected to have, that is the machine itself and all wheels, and a crib. My particular task was to discover whether the inner setting (wheel order) and stecker could be recovered from a crib ob 25 letters. I started with no knowledge of the Enigma machine, and I was able to show that this was possible. It is however only feasible if the wheel in the right hand position has one turn-over only. If you have in the right hand position a wheel with more than one turn-over, the problem becomes very difficult.

7. I first investigated the wiring of an individual wheel. [He made the diagram I(a), See end of report--from which he built up later a rod square, diagram I(b)]. My studies were not entirely theoretical

8. It is assumed that all 26 letters of the crib which are used are encyphered with only the right hand wheel moving, the other wheels remaining fixed. This assumption is necessary, since if the crib involves a turnover the effect is the same as a right hand wheel having 2 turnovers. Although theoretically soluble, the work involved in this case would be very heavy.

9. It is first necessary to do a single letter frequency count of the 52 letters, 26 of the crib, and 26 of the cypher text. The letter A is relatively common in this example. Look for one or more instances in which any particular pair of freqent letters occur as constatations. In the example AN pairing occurs, and A, N are taken as the letters to start from. For these two, and all other letters in turn, an analysis is made, giving the position of each occurrence and the letter paired to it. [See diagram II(b)]

10. I can now start investigation of the stecker. In establishing the stecker there are 26 possibilities for A. For each of these 26 possibilities there are a further 24 possibilities for N. It is necessary to carry out over 600 tests on this basis. First assume A steckered to A and N steckered to B. Assume also that the first letter of the crib is encyphered with the right hand wheel in position 1.

11. On pressing the letter A in position 1 (with unsteckered machine), the current enters the later wheels at point 5. This is read from the rod square. The relevant columns of the rod square are entered in the analysis of constatations (see diagram II(b)). For every occurrence of A, record in a table (diagram II(c)) the point at which current enters the later wheels. Then for B, using row N of the rod square since N is steckered to B, we get from constatation BT at 7 the entry 17 under 7. Similarly for N.

12. From the AN constatation we discover that there must be a connection (through the remaining wheels and reflector) between 17 and 4, if all assumptions madd up to now are correct. This connection, obtained at position 21, must continue to exist throughout the encypherment as the other wheels do not move. Then of course at every other point where we have 4 we can put 17.

13. In particular, in position 6 we have NF pairing. As N is steckered to B, current enters middle wheel at 4, and 4 is connected to 17, which in column 6 of the rod square (or from diagram II(b)) is opposite F. Therefore F self-steckered is a consequence of our hypotheses. We do not particularly look for self-stecker, because it hinders rather than assists.

14. Working on, we find that G is steckered to R, using column 12. At point 12 we have NR pairing. As N is steckered to B we get current entry 4; looking for 17 in the column we find it opposite G, giving G/R. We have thus produced 2 new stecker pairings.

15. Now use the table for F, to put further entries into the table of rod pairings. [He called this the reconstructed stecker table.] As F is self-steckered, the entries are to be taken from row F. In position 5 we get 12, and in 11 we get 20. It now turns out that in position 5 we have deduced 2 connected to 12, and in position 11, 12 connected to 20. These are incompatible, and therefore one or more of the assumptions which we have made must be wrong. An incompatibility of this type may turn up at the beginning or late in the work, but usually early on.

16. Our new assumption for the stecker is that N is steckered to C instead of B. It is necessary to go on making assumptions, until we

17. We must now repeat the tests assuming a new wheel position. This of course takes 26 more days or 26 more men. If we still get no answer, we must repeat for all the wheels, on the assumption that the original right hand wheel tried was wrong.

18. In the case of a wheel with 2 turnovers it is very difficult to build up the stecker completely. The table of rod pairings must be built up in two halves, because the connections will be different when the middle wheel has moved. The labour is heavy. If the wheel has only one turnover, we have a stretch of 26, in which there will be repeats between the rod pairings involved, sometimes 4 or 5 occurrendes of a pairing. On the basis of a stretch of 13 only it is unlikely that they will repeat more than once.

19. Suppose we have used all the material available in the 25 letter crib, without reaching a contradiction, then a further assumption must be made. Find what common letters are unaccounted for in the stecker obtained, for example K. Now assume a new stecker for K, first K steckered to D. With this assumption the table either fills itself up easily, or a contradiction is immediately apparent. You cannot say that the initial assumptions are wrong until all remaining possibilities for K have been tried out and failed.

20. As far as letters not in the original crib or cypher text are concerned, it is not necessary to extend the test to them since towards the end the process will be very "piecy" in any case. You can of course include in the stecker table letters which are not in either the crib or cypher text, if they are steckered to letters which are.

21. If this is done with every wheel in the right hand position in turn, then the one which gives the right answer must be the right hand wheel of the inner setting which we are attempting to recover. Connections through the remaining wheels are constant since they do not move. We must now establish the order of the remaining wheels.

22. The whole problem was tackled on the assumption of a 4-wheel enigma, although up to this point it does not of course matter how many wheels there are. If the wheel in the right hand position has more than 2 turnovers, the problem becomes impossible. The Naval Enigma wheels had either 1 or 2 turnovers. There was talk of using up to 26 turnovers for the right hand wheel. All wheels would be adjustable, but only the right hand wheel would have more than the ordinary number of turnovers.

23. With the second wheel from the right the basic problem is the same. It can only be studied when it moves alone, the other wheels remaining stationary. Perhaps 10 or 13 letters might be sufficient.

24. The number of theoretical electrical connections is 25 x 23 x ..... x 3 x 1 = 8 x 10^{12} approx. The practical possibilities for rod pairings on the 4-wheel enigma is

56 x 2 x 2 x 26^3 = 4 x 10^6 approx.

(There are 2 possibilities for UKW, 2 for Zusatzwalze, and the left hand and middle wheels are 2 out of 8 wheels available.) Thus the practical possibilities are a small fraction of the theoretical possibilities.

25. The following stages in the process were not carried out in practice, but the theoretical calculations were done. In practice Hollerith machinery would be used. For every one of the 4 x 10^6 possibilities construct a Hollerith card, and sort by rod pairings, with all wheel orders together. When this catalogue has been made, go back to the table giving ingoing and outgoing course of the current. Suppose the table gives

26. After 5 or 6 processes 4,000,000 cards are probably reduced to 1 card. This will then give the wheel order, and the position of the wheels.

27. With a 3-wheel Enigma the number of practical possibilities is only 56 x 2 x 26^2 = 70,000. Thus only 70,000 instead of 4,000,000 cards are required.

28. The problem set to me was to determine whether the inner setting could be determined on a crib of 25 letters. By the above process I showed that it could, given certain favourable circumstances.

29. No effort was made to try out the theory in practice on a three-wheel Enigma. The Hollerith catalogue once made is of course effective for the life of any one set of wheels. The enemy could have produced the 70,000 cards at the beginning of the war and this catalogue would have been valid throughout the life of the three-wheel Enigma. The first Hollerith card sorting process would take 200 machine/hours, the second only 8 machine/hours, and so on.

30. The method was theoretically applicable with a crib of as few as 13 letters, but thousands of personnel would be necessary.

31. The official reaction to the findings of the investigation was the immediate decision that only wheels with two turnovers should be allowed to be used in the right hand position. This was introduced at the beginning of December 1944. It reduced the possible permutations of the wheel order, but increased the security of the machine against this particular weakness.

32. The view of the German Army was that their Enigma was theoretically soluble. The four-wheel Enigma was not considered theoretically soluble and the Army were astonished at the Navy's view based on this investigation."

---

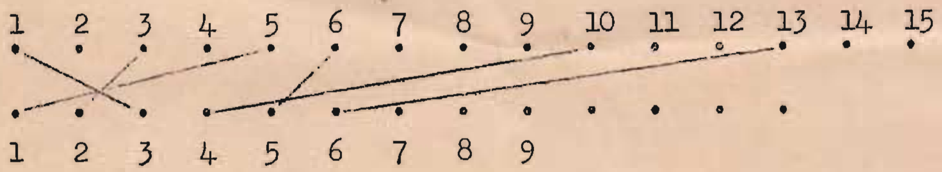
33. TRANOW was asked whether any investigation into the security of the Enigma machine had been made before July 1944. He replied that Fregatten Kapitan SINGER of 4 SKL II was responsible for current monitoring and surveillance of German traffic, but as he had already pointed out, these sort of people were no use -- the only effective action was to do what the enemy may be expected to do, that is, a first class cryptanalytic attack.

34. The results of this work were not considered in their application to Typex. Before it could have been applied, it would have been necessary to have both the machine and the wheels, and even then the work would have assumed vast proportions.

35. FROWEIN finished his researches by calculating a method recovering wheel wirings, assuming wheels uncompromised by capture. This could be done with larger crib material, but no detailed investigation on this was made. Three or four cribs of 52 or 78 letters would be required. There was considered to be little point in pursuing this further as although the wheels were in enemy hands, they could not be changed.

36. During the course of the interrogation it emerged that FROWEIN had been awarded the War Merit Cross for his research on the Enigma together with his other cryptographic work.

I(a)



I(b)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	5	2	25	7	2	8	3	10	15	7	12	15	3	6	24	15	4	11	22	6	17	3	11	21	23	9
B	3	26	8	3	9	4	11	16	8	13	16	4	7	25	16	5	12	23	7	18	4	12	22	24	10	6
C	1	9	4	10	5	12	17	9	14	17	5	8	26	17	6	13	24	8	19	5	13	23	25	11	7	4
D	10	5	11	6	13	18	10	15	18	6	9	1	18	7	14	25	9	20	6	14	24	26	12	8	5	2
E	6	12	7	14	19	11	16	19	7	10	2	19	8	15	26	10	21	7	15	25	1	13	9	6	3	11
F	13	8	15	20	12	17	20	8	11	3	20	9	16	1	11	22	8	16	26	2	14	10	7	4	12	7
G	9	16	21	13	18	21	9	12	4	21	10	17	2	12	23	9	17	1	3	15	11	8	5	13	8	14
H	17	22	14	19	22	10	13	5	22	11	18	3	13	24	10	18										10
I	23	15	20	23	11	14	6	23	12	19	4	14	25	11	19											18
J	16	21	24	12	15	7	24	13	20	5	15	26	12	20												24
K	22	25	13	16	8	25	14	21	6	16	1	13	21													17
L	26	14	17	9	26	15	22	7	17	2	14	22														23
M	15	18	10	1	16	23	8	18	3	15	23															1
N	19	11	2	17	24	9	19	4	16	24																16
O	12	3	18	25	10	20	5	17	25																	20
P	4	19	26	11	21	6	18	26																		13
Q	20	1	12	22	7	19	1																			5
R	2	13	23	8	20	2																			6	21
S	14	24	9	21	3																			7		3
T	25	10	22	4																			8			15
U	11	23	5																			9				26
V	24	6																			10				1	12
W	7																			11				2	13	25
X	18																		12				3	14	26	8
Y	21																	13				4	15	1	9	19
Z	8																14				5	16	2	10	20	22

II(a)

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1
A	N	K	U	N	F	T	S	C	H	A	R	N	H	O	R	S	T	S	T	A	V	A	N	G	E	R
R	L	D	K	F	N	B	Y	G	L	F	N	K	O	L	S	K	V	N	D	N	A	F	L	A	L	B

II(b)

			A								N				B				F	
	R	F	N	V	F	G	L	F	F	R	K	S	A	L	T	N	N	A	.	. .
	1	11	21	22	23	25	2	5	6	12	13	19	21	24	7	5	6	11		
a	5	12	17	3	11	9	2	2	8	15	3	22	17	21	3	2	8	12		
b	3	16	4	12	22	6	26	9	4	4	7	7	4	24	11	9	4	16		
c	1	5	13	23	25	4	9	5	12	8	26	19	13	11	17	5	12	5		
d	10	9	24	26	12	2	5	13	18	1	18	6	24	8	10	13	18	9		
e	6	2	1		9		12	19	11	19	8		1		16	19	11	2		
f	13	20	14				8	12	17	9						12	17	20		
g	9		11					18		17						18		10		
h	•															22				
i	•																			
j	•																			
k	•																			
l																				
m																				
n																				
o																				
•																				
•																				
•																				

II(c)

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
5	26			2	4	19				12	4	7						7		17	3	11	24	9	
				12	17					20	17									4					

Stecker A/A, N/B
giving F/F, G/R